

CCTV ADMINISTRATOR'S CHECKLIST

Establish CCTV exploration committee

Include representatives from the police, homeland security, emergency management, academic, legal, political, business, civic, religious, civil liberties protection, technical field of video surveillance, etc.

Is video surveillance the best method to address the problem?

Determine if CCTV is the most effective/efficient method to address the problem?

Evaluate whether townwatch programs, improved lighting, curfew legislation, hardening of potential targets, integration of private security with public safety, restricting access to high risk locations, redeployment of police resources, etc. would be better at addressing the problem

Identify other cities and agencies using CCTV and initiate contact to identify positives and negatives of those systems

Decide whether sustainability will become an issue

How long will the commitment of personnel be able to be maintained?

How long will funding be able to be maintained?

How long will public and political support be maintained?

Explore funding possibilities

Identify and apply for local, state and federal grants

Solicit corporate sponsors

Recruit organizations and community groups wishing coverage and willing to pay for equipment purchase and installation

Develop collaborative operation

Involve utility providers, critical infrastructure locations, schools, high volume public areas, traffic control, crime suppression/detection, other city service agencies etc.

Excerpt from thesis authored by Thomas J. Nestel, III and available via:

https://www.hsdl.org/homesec/docs/theses/06Mar_Nestel.pdf&code=c652f57a750279b26159c07bb6989fd6

Involve the community

Consider introducing ballot question requesting permission to implement CCTV surveillance of public domain

Hold town meetings to introduce idea and garner support

Conduct an outreach effort to formal/informal organizations including business, civic, professional, educational, religious, political, labor etc.

Locations for cameras

Decide whether camera locations will be confidential or subject to full disclosure

Conduct longitudinal review of crime data

Utilize hazard analysis to identify high risk locations

Commit to locations that provide funding

Use consultant's input to assist in identifying the most effective locations

Post signs notifying public in video surveillance areas

Develop registration and licensing process for public domain

Require private industry to answer the following questions:

- What will the system watch?
- Who will be the system administrator?
- Why does management feel surveillance system is necessary?
- What is the coverage area?
- What are the system capabilities?
- How will abuse be prevented?
- How long will images be retained?
- What is the image release policy?

Establish regulations for private industry to adopt and provide to company's seeking registration and licensing

Require yearly renewal that evaluates whether the need for surveillance still exists

Enable spot checks by government entity

Enable fines and system termination for violations

Excerpt from thesis authored by Thomas J. Nestel, III and available via:

https://www.hsdl.org/homesec/docs/theses/06Mar_Nestel.pdf&code=c652f57a750279b26159c07bb6989fd6

Establish procedure for response to suspicious or illegal behavior

Decide whether system will serve preventive or evidentiary purpose:

- If preventive, system operators should have protocol regarding what to do for observations of suspicious or illegal behavior
- If evidentiary, legal review should be conducted to determine if non-automated systems should follow preventive system protocols
- If evidentiary, protocol for notifying police upon initiation of illegal behavior and method for transferring images to investigators

Mechanize operations

Consider utilizing cameras that automatically rotate

Consider utilizing software that conducts face recognition

Consider utilizing software that conducts license tag comparisons

Consider utilizing software that identifies and locates gunfire

Consider utilizing software that alerts system operators when traffic stops for extended periods of time or when items are left unattended in a public area

Consider utilizing software that alerts system operators when movement occurs in restricted or high threat areas

Consider utilizing software that blocks out windows, fenced-in yards, and special locations such as health clinics, etc.

Adequate supervision

Ensure that a supervisor is always on duty whenever cameras are monitored by human operators

Restrict access to the video center and image storage location

Establish control log that documents the names and hours of personnel working each shift; names, times and purpose of entry into the center by non-assigned personnel; requests for images; and noteworthy incidents

Excerpt from thesis authored by Thomas J. Nestel, III and available via:

https://www.hsdl.org/homesec/docs/theses/06Mar_Nestel.pdf&code=c652f57a750279b26159c07bb6989fd6

Confidentiality agreement

Require all personnel assigned to any element of the surveillance system operation to review and sign a confidentiality agreement

Agreement should include a clause that the employee has received, reviewed and understands the department's written policy regarding surveillance system operations

Agreement should include any laws specifically adopted to regulate surveillance system operations

Agreement should include the warning that violations will result in termination and possible civil/criminal action

Chain of custody for images

Images should have electronic protection such as, watermarking or encryption

Images should be stored in secure location and any access to images should be recorded

Release of images should only occur upon written request through a designated chain of command

Release of images should be limited to:

- assist in terrorism/criminal investigation
- evidence indicating the commission of a crime
- training for first responders

Creation of legislation

Engage lawmakers and guide in the establishment of legal standards for the operation of surveillance systems monitoring the public domain

Establish legislation with penalties for violations including imprisonment and fines

Restrict the release of images except as described above

Develop a minimum and maximum time frame for image retention

Prohibit the interception of image transfer from wireless, intranet or other electronic platforms

If camera location confidentiality is determined to be necessary, establish legislation prohibiting the release of such information

Excerpt from thesis authored by Thomas J. Nestel, III and available via:

https://www.hsdl.org/homesec/docs/theses/06Mar_Nestel.pdf&code=c652f57a750279b26159c07bb6989fd6

Training

Develop special training specifically for surveillance system operations

Training should be provided for all levels of system operations from technical personnel to administrator

Training should include Constitutional issues, case law, search and seizure regulations, state and local legislation, ethical considerations, and departmental policy

Training should occur prior to assignment in surveillance system operations and yearly to reinforce the importance of acceptable behavior

Written policy

Develop a written policy that clearly defines the mission of the surveillance system

Identify the system administrator responsible for all operational and administrative elements

Explain the system capabilities

Present parameters for system use, image retention and release, and access to video center and image storage location

Note the legal and departmental restrictions for surveillance system operations

Publicity

In order to develop and establish the deterrence factor of behavior control, the news media should be a partner in reporting the implementation of the system and any subsequent success stories or requests for help in identifying suspects

Excerpt from thesis authored by Thomas J. Nestel, III and available via:

https://www.hsd1.org/homesec/docs/theses/06Mar_Nestel.pdf&code=c652f57a750279b26159c07bb6989fd6